Let $e_Z : Z_1 \times Z_2 \to T$ be a pairing on elliptic curves $Z \in \{X, Y\}$ with slooow dual isogenies $\phi : Y \to X$ and $\phi^* : X \to Y$.

See: `https://eprint.iacr.org/2019/166`

$$e_Y\big(H_1(\texttt{seed}), u\overbrace{\phi G_2}^{const}\big) = s = e_X\big(\overbrace{\phi^* H_1(\texttt{seed})}^{VDF}, \underbrace{uG_2}_{U}\big)$$

Anyone sends ciphertexts $\big(U, E_s(\texttt{vote})\big)$,
after `seed` revealed but well before $\phi^* H_1(\texttt{seed})$.

Moral: ASICs for RSA are not the best use for 30 millon USD.